

# Small Businesses: Be Alert to Identity Theft

Small business identity theft is a big business for identity thieves. Just like individuals, businesses may have their identities stolen and their sensitive information used to open credit card accounts or file fraudulent tax returns seeking bogus refunds. To mark "National Tax Security Awareness Week," the Delaware Division of Revenue, along with the IRS and the nation's tax industry have joined together to warn small businesses to be on-guard against a growing wave of identity theft against businesses and employers.

In the past year, the Internal Revenue Service noted a sharp increase in the number of fraudulent Forms 1120, 1120S and 1041 as well as Schedules K-1. The fraudulent filings include forms filed relating to partnerships, estates and trusts. Identity thieves are displaying a sophisticated knowledge of the tax code and industry filing practices as they attempt to obtain valuable data to enable them to file fraudulent returns.

Identity thieves have long made use of stolen Employer Identification Numbers (EINs) to create fake Forms W-2 that they file with fraudulent individual tax returns seeking refunds. Fraudsters also used EINs to open new lines of credit or obtain credit cards. Now, they are using company names and EINs to file fraudulent returns for the businesses themselves.

As with fraudulent individual returns, there are certain signs that may indicate identity theft. Those filing returns for corporations, partnerships, estates or trusts should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- Extension to file requests are rejected because a return

with the Employer Identification Number or Social Security number is already on file;

- An e-filed return is rejected because a duplicate EIN/SSN is already on file with the IRS;
- An unexpected receipt of a tax transcript or IRS notice that doesn't correspond to anything submitted by the filer;
- Failure to receive expected and routine correspondence from the IRS because the thief has changed the taxpayer's address.

## **New Procedures to Protect Businesses in 2018**

The Division of Revenue, the IRS, and software providers share certain data points from returns, including business returns, which help identify a suspicious filing. Delaware and the IRS are asking that businesses and tax practitioners provide additional information that will help verify the legitimacy of the tax returns they file.

For 2018, the "know your customer" procedures that are being put in place include the following questions:

- Authorized signer – Confirm the name and SSN of the company executive authorized to sign the corporate tax return;
- Payment history – were estimated tax payments made? If yes, when were they made, how were they made, and how much was paid?
- Parent company information – is there a parent company? If yes, what is the name of the parent company?
- Deduction information – Provide additional information based on deductions claimed;
- Filing history – has the business filed Form(s) 940, 941 or other business-related tax forms?

Individuals operating as sole proprietorships who file Schedule C with Form 1040 and partnerships that file Schedule

K-1 with Form 1065 also will be asked to provide additional information items, such as a driver's license number. Providing this information will help Delaware and the IRS identify suspicious business-related returns.

For small businesses looking for a place to start on security, the National Institute of Standards and Technology (NIST) has produced [Small Business Information Security: The Fundamentals](#). NIST is the branch of the U.S. Commerce Department that sets information security frameworks followed by federal agencies. The United States Computer Emergency Readiness Team (US-CERT) has created [Resources for Small and Midsize Businesses](#).

Take the steps recommended by cyber experts to protect your business, and visit the [Identity Protection: Prevention, Detection and Victim Assistance](#) for more information about business-related identity theft.